ICT Acceptable Use Policy (AUP)

Version Number: 1.0

Introduction

It is the responsibility of all the users of information and communication technology (ICT) facilities and services of Jigme Namgyel Engineering College (JNEC) to read and understand this policy.

This policy may be updated from time to time without user’s consent, in order to comply with legal and policy requirements.

1. Purpose

The purpose of this document is to outline the acceptable and prohibited use of its ICT facilities and sanctions for non-compliance. The policy addresses the need to protect the College and its students, staff and its associates, from illegal or damaging use of technology by individuals, either knowingly or unknowingly.

2. Scope

2.1. ICT facilities encompass (but are not restricted to) the following services provided by the College and third parties on its behalf:

2.1.1. network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers;

2.1.2. network services, including (but not exclusively) Internet access, web services, email, wireless, messaging, file store, printing, CCTV;

2.1.3. College owned computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, smart phones, tablets, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices;

2.1.4. software and databases, including applications and information systems, virtual learning and videoconferencing environments, ICT laboratories, software tools, information services, electronic journals & e-books.

2.2. The College may make changes to the Policy at any time. Users will be notified of the changes.

3. Policy Statements

Any individual using the ICT facilities is deemed to have accepted this Policy and is bound by it.

ICT facilities are provided to users primarily for the College business purposes to support teaching, learning, research and professional & administrative activities. The College’s primary purpose of ICT facilities take priority over any personal use.

4. Acceptable Use

All users of the ICT facilities must comply with the following principles:

4.1. The College expects users to use the ICT facilities and access to the Internet in a responsible manner in accordance with this policy and all applicable laws of Royal Government of Bhutan.

4.2. Users must also comply with the regulations and policies that are applied by Royal University of Bhutan in respect of the ICT facilities;

4.3. Each user is issued with a valid username and password which must be used to authenticate and gain access email, internet and other online services. The password must be kept confidential and must not be shared with anyone else;

4.4. All Users are responsible for all activity that takes place under their usernames and must not allow anyone else to access the ICT facilities using their usernames and passwords. Access to the ICT facilities using someone else's user name and password is prohibited.

4.5. All Users should be courteous and considerate of others when using the ICT facilities;

4.6. The College expects all staff and students to utilize the official email accounts as the primary mechanism for official correspondence. All staff and students are expected to adhere to the College's Email Policy while using official email accounts.

4.7. Comply with all relevant copyright legislation, licenses and agreements for software and electronic information resources when accessing and connecting to College ICT facilities;

4.8. Obtain authorization for installing software on College owned computers from Information Technology Service Unit (ITSU);

4.9. Obtain authorization for connecting any personally owned ethernet switch, wireless router and other network devices from ITSU;

4.10. Users should make all reasonable efforts to send data that is 'virus free' and not open email attachments or click on links sent by unsolicited or untrusted sources;

4.11. Users should ensure any personally owned computer (with appropriate authorization from ITSU) used to access College ICT facilities have anti-virus programs thereby protecting the College network as much as possible from accidental or premeditated virus and hacking attempts and attacks;

4.12. Users will be solely responsible for all claims, liabilities, damages, costs and expenses suffered or incurred by the College which result from their use of the ICT facilities in contravention of this Policy;

4.13. Users should report any technical problems, requests or concerns regarding a suspected policy breach directly to the ITSU.

5. Not Acceptable Activity

Users may not use College ICT facilities to:

5.1. cause the good name & reputation of the College or any part of it to be damaged or undermined by carrying out, facilitating or furthering inappropriate, criminal or any other activity that conflicts with all applicable laws in the Country and / or College policy or regulations;

5.2. carry out any personal business, gambling or non-academic related commercial purpose;

5.3. access any of the College owned system by circumventing the network authentication process;

5.4. sell or redistribute any part of the ICT facilities

5.5. continue to use any networked hardware or software after being identified as causing disruption to the correct functioning of the College ICT facilities;

5.6. deliberately or unintentionally receive, access, create, change, store, download, upload, share, use or transmit:

5.6.1. any illegal, obscene or indecent images, data or other material;

5.6.2. any infected material or malicious code (including, but not restricted to, computer viruses, spyware, trojan horses and worms) whether designed specifically or not, to be destructive to the correct functioning of computer systems and networks;

5.6.3. any material which the College may deem to be advocating, inciting or encouraging illegal activity, threatening, harassing, defamatory, bullying, abusive, offensive or otherwise causing annoyance or inconvenience;

5.6.4. any material that infringes the copyright or confidentiality of another person or institution, or infringes the copyright laws (including but not exclusive to music, films, radio and TV);

5.7. share links to websites which have pornographic or inappropriate material, or which publish defamatory materials or discriminatory statements;

5.8. falsify emails to make them appear to have been originated from someone else, or send anonymous messages without clear indication of the sender;

5.9. carry out activities that criticize or harm individuals or that violate the privacy of other individuals;

5.10. gain or attempt to gain unauthorized access to facilities or services via the College ICT facilities, using automated processes or otherwise;

5.11. allow, incite, encourage or enable others to gain or attempt to gain unauthorized access to, or carry out unauthorized modification to the College's or others' ICT facilities;

5.12. deliberately or unintentionally use file-sharing systems (sometimes known as P2P or peer-to-peer) to download or upload copyright material without the copyright owner's permission (including but not limited to music, films, games, and software);

5.13. connect any non-approved or personally owned ICT equipment to the College physical (wired) network points without authorization from ITSU;

5.14. intentionally or unintentionally transmit unsolicited or unauthorized commercial or advertising material, unsolicited e-mail (spam), chain letters, hoax virus warnings, pyramid letters or other junk mail of any kind;

5.15. install any software in any of the College owned computers without authorization of ITSU.

5.16. save or share any College owned confidential information.

6. Enforcement of the ICT Acceptable Use Policy

6.1. Monitoring

All email, internet use and other online ICT tools usage is logged, and may be subject to automated monitoring. Monitoring may be carried out in compliance with applicable obligations under National Law (and associated regulations) for the purposes of:

6.1.1. preventing or detecting criminal activities

6.1.2. investigating or detecting unauthorized use of the College's ICT facilities

6.1.3. ensuring effective system operation.

Records of all ICT activity will be retained and in the event of security vulnerability reports or copyright infringement notices, routine investigation of network activity logs will be carried out.

The College reserves the right to inspect any items of College owned computer equipment connected to the network. Any ICT equipment connected to the College's network can be removed if it is deemed to be breaching policy or otherwise interfering with the operation of the network.

6.2. Incident reporting procedures

Information security events or any suspected breaches of this policy should be reported immediately to the College Management or ITSU.

6.3. Misuse and Sanctions

Individuals violating any of the practices or procedures set out in this policy shall be held liable and cases will be dealt depending upon the nature of the offence. The case will be investigated by the team from IT Service Unit of the college and report the matter to the college administration for application of any standing sanctions with reference to the existing policies of the College.

Where there is evidence of a criminal offence, the issue will be reported to the Police (or relevant statutory body) for their action.

7. Disclaimer

The College provides the ICT facilities for the benefit of itself and its staff, students and associates and no guarantee is given that use of the ICT facilities will be fault-free, uninterrupted and secure.

Users of the ICT facilities understand and agree that the College will not be liable to them for any damages, cost or losses arising out of, or any way connected with the use of the ICT facilities.

8. Related Documentation

8.1. College Policy

The following Students Code of Conduct and Ethics is available at : https://www.jnec.edu.bt/en/student-code-of-conducts-ethics/

8.2. External documents

The overall ICT policies are governed by Department of Information Technology and Telecom (DITT) policies https://www.dit.gov.bt/ict-policies

G Suite for Education, Code of Conduct available at https://gsuite.google.com/terms/education_privacy.html